METHOD AND APPARATUS FOR TRACING A DENIAL-OF-SERVICE ATTACK BACK TO ITS SOURCE

ABSTRACT OF THE DISCLOSURE

A backtracking method, program and unit for tracing a denial-of-service attack on a victim machine, such as a server, back towards its source. The backtracking unit includes a data processor that is responsive to a traceback computer program stored on a computer-readable media for receiving a first input parameter of an IP address (v) of the victim machine and a second input parameter of an IP address (r) of a router that is immediately upstream of the victim machine. The traceback computer program controls the operation of the data processor to determine a set of routers that are neighbors (n) of r and, for each neighbor n of r, to determine if r is n's next-hop for traffic addressed to v, where node n's next-hop for traffic addressed to v is the IP address of the node that n will forward a packet if the destination address in the packet is v. The traceback computer program further controls the operation of the data processor, for the case where r is not n's next-hop for traffic addressed to v, to skip over n and to query the next neighbor of r, while for the case where r is n's next-hop for traffic addressed to v, to determine an amount of traffic that n is forwarding to r that is addressed to v or to a network to which v is connected. After determining the identity of the neighbor n of r that is the principal source of packets flowing to r that are addressed to v, the data processor continues further upstream from the determined neighbor n of r that is the principal source of packets flowing to r that are addressed to v to continue to traceback through interconnected routers until a source of denial-of-service attack packets to v is determined. The data processor operates to send at least one query to r, such as a Simple Network Management Protocol (SNMP) query, to obtain information from a MIB that stores IP addresses of routers that are neighbors of r. The data processor also operates to send at least one query to an IP Forwarding Table MIB of router n. The data processor, while determining an amount of traffic that n is forwarding to r that is addressed to v, operates under control of the traceback computer program to send a first message to a neighbor router n instructing router n to count the number of packets that it is sending to router r that are addressed to v, and further operates to send a second message to router n to query router n as to how many packets it has sent to router r addressed to v.